

# A Survey of Black and Gray Hole Attacks in Wireless Mobile Ad Hoc Networks

Divya S<sup>1</sup> Chandrasekar A<sup>2</sup>

<sup>1</sup>PG Scholar <sup>2</sup>Associate Professor

<sup>1,2</sup>Department of Computer Science & Engineering

<sup>1,2</sup>SNS College of Technology, Coimbatore-35, Tamilnadu, India

*Abstract*— A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. MANET is group of large independent wire nodes interconnecting each other on peer to peer basis in an environment without any infrastructures. There are different attacks against the routing protocol in ad hoc networks. These attacks may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at impeding the formation of the network, making legitimate nodes store incorrect routes, and more generally at perturbing the network topology. In this paper analysis, different type of black and gray hole attack detection techniques and algorithms in existing paper. A packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as traceroute. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. In this paper a survey on different detection and prevention techniques for the black hole and gray attack in MANET is presented.

**Key words:** Mobile ad-hoc Networks, Packet Drop, Black Hole attacks, Gray Hole Attacks

## I. INTRODUCTION

Infrastructure-based systems that use as cellular or WiFi technology utilize a central 'hub' node to deliver high speed connectivity and good Quality of Service (QoS) to the user. Removing this infrastructure and adding mobility, coupled with time varying connectivity profile without adversely affecting the user's QoS is the formidable challenge faced by developers of Wireless Mesh Networking (also called MANET, or Mobile Ad hoc Networking) systems. A MANET system is a group of mobile (or temporarily stationary) devices which need to provide the ability to stream voice, data, and video between arbitrary pairs of devices utilizing the others as relays to avoid the need for infrastructure.

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self- configuring network of mobile devices connected by wireless links. In other

words, a MANET is a collection of communication nodes that wish to communicate with each other, but has no fixed infrastructure and no predetermined topology of wireless links. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Individual nodes are responsible for dynamically discovering other nodes that they can directly communicate with. Due to the limitation of signal transmission range in each node, not all nodes can directly communicate with each other. Each node must forward traffic unrelated to its own use, and therefore be a router.

Ad hoc networks are suited for use in situations where infrastructure is either not available or not trusted, such as a communication network for military soldiers in a field, a mobile network of laptop computers in a conference or campus setting, temporary offices in a campaign headquarters, wireless sensor networks for biological research, mobile social networks such as Facebook, My Space and Twitter, and mobile mesh networks for Wi-Fi devices.

In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nearby nodes and how to reach them, and may announce that it can reach them too. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations.

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To thwart or prevent such attacks, it was necessary to employ authentication mechanisms that ensure that only authorized nodes can inject traffic into the network. Even with authentication, these networks are vulnerable to packet dropping or delaying attacks, whereby an intermediate node drops the packet or delays it, rather than promptly sending it to the next hop. Some behavior-based detection techniques have been developed to counter such attacks in which a node overhears communication in the wireless neighborhood and determines if a neighbor is behaving correctly, i.e., forwarding the packet toward the intended recipient promptly.

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks. There are various mechanisms have been proposed for solving single black hole attack in recent years.

However, many detection schemes are failed in discussing the cooperative black hole problems.

## II. ROUTING PROTOCOLS IN MANET

A Mobile ad-hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like-packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network relay on one another in forwarding a packet to its destination, due to the limited range of each node's wireless transmissions.

### A. Table-driven or Proactive Protocols

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include: Destination-Sequenced Distance Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP), and Optimized Link State Routing (OLSR).

### B. On-demand or Reactive Protocols

A different approach from table-driven routing is reactive or on-demand routing. These protocols depart from the legacy Internet approach. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Representative reactive routing protocols include: Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR).

### C. Hybrid Routing Protocols

Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently. For example, reactive routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. The performance of either class of protocols degrades when the protocols are applied to regions of ad hoc networks space between the two extremes.

## III. DIFFERENT TYPE OF ATTACKS

In MANETs, the wireless channel is accessible to all the nodes, both legitimate network users and malicious attackers. Moreover, every node is capable of functioning as a router. This is in direct contrast to wired networks that have dedicated routers. From a security perspective, we can say that there is no clear line of defense. There is no well-defined place where traffic monitoring or access control mechanisms can be deployed. Because of these reasons,

MANETs are particularly vulnerable to security attacks by malicious nodes.

### A. Passive Attacks

In such an attack, the enemy node does not disturb the connection in any way. It just eavesdrops on the network and collects data flowing through it. This means that the data is not confidential. This type of attack is usually difficult to detect, as the performance of the network does not change. In general, encryption is used to mitigate such attacks.

### B. Active Attacks

In this form of attack, the intruding node actively interferes in the operation of the network. This might include actions such as dropping of packets, flooding the network with route requests and re - routing the packets. Active attacks are referred to as 'internal attacks' or 'external attacks' based on whether the intruding node belongs to the same network or a foreign network. Multi-hop connectivity is provided in MANETs by first ensuring one hop connectivity through link layer protocols (ex. MAC) and then by extending connectivity to multiple hops through network layer routing and data forwarding protocols (ex. ad hoc routing protocols). The logic of routing is essentially implemented in the network layer. Some of the active attacks at the network layer are:

### C. Black Hole Attack

Here, an enemy node advertises that it has the shortest path to any required destination. This causes all other nodes to direct their data packets to this node. Then the malicious node can either drop all the packets or routes the packets outside the network.

### D. Wormhole Attack

This is a routing attack caused by an enemy node in a network that redirects the packets that it receives outside the network to another enemy node. After the second node finished snooping on the packet, it is re - routed into the network.

### E. Denial of Service

In this case, an enemy node might flood the network with unnecessary route request problems. This leads to congestion in the network, leading to inaccessible resources for other nodes.

Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks.

In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability. the resource constraints on nodes in ad hoc

networks limit the cryptographic measures that are used for secure messages. Thus, it is influence to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Finally, lack of cooperation and constrained capability is common in wireless MANET which makes anomalies hard to distinguish from normalcy. Security Approaches in MANETs

#### IV. SECURITY APPROACHES IN MANTES

##### A. Proactive

This approach attempt to thwart security threats in the first place through various cryptographic techniques.

##### B. Reactive

First detect the threat react accordingly. Due to the absence of a clear line of defense, a complete security solution for MANET should involve both approaches. Prevention can be achieving by secure Ad-hoc routing protocols that prevent the attackers form installing incorrect routing states at other nodes.

Because the wireless channel is open, each node can perform localized detection by overhearing on going transmission and evaluating the behaviour of its neighbours but its accuracy is limited by a number of factors such as channel error, interference and mobility. A malicious node may also abuse the security solutions and intentionally censure legitimate nodes, in order to address such issues, the detection results at individual nodes can be integrated and refined in a distributed manner to achieve consensus among a group of nodes. An alternative approach relies on explicit acknowledgement from the destination and/or intermediate nodes to the source so that the source can figure out where the packet was dropped. Once a malicious node is detected certain actions are triggered to protect the network from future attacks launched by this node the reaction component is related to the prevention component in the security system. Once multiple nodes in a local neighbourhood have reached consensus that one of their neighbours is malicious, they collectively revoke the certificate of the malicious node. The malicious node is isolated in the network as it cannot participate in the routing or packet forwarding operations in the future. The path rather allows each node to maintain its own rating for every other node it knows about. A node slowly increases the rating of well-behaved nodes overtime, but dramatically decreases the rating of a malicious node that is detected by its watchdog. Based on rating source always selects the path with the highest average rating.

#### V. EXISTING SOLUTION FOR BLACK HOLE AND GRAY ATTACK

M. Chuah et. al., [1] In this paper author describe traditional adhoc routing schemes do not work well in sparse ad hoc networks. So, in this paper proposed a ferry based intrusion detection and mitigation (FBIDM) scheme for sparsely connected ad hoc networks that using Prophet routing protocols Via simulations. The drawbacks of this paper if nodes cannot hear their neighbors forwarding communications due to hidden terminal problem or the use of different modulation schemes to applied so it will take high computation time.

Y. Ren et. al., [2] In this paper author proposed a mutual correlation detection scheme (MUTON) for talking these insider attacks. MUTON takes into consideration of the transitive property when calculating the packet delivery probability of each node and correlates the information collected from other nodes is used for sending the packet to neighbor node. The drawbacks of this paper High node overheard and insufficient transmission power.

Z. Gao et. al., [3] In this paper author proposed iTrust is presenting a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically examination. This model iTrust as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. The drawbacks of this paper Difficulty to predict mobility patterns and Costly in terms of transmission overhead and verification cost.

N. Li and S. K. Das [4] In this paper, proposed and study the design a trust-based framework to more accurately evaluate an encounter's delivery competency, which can be flexibly integrated with a large family of existing data forwarding protocols designed for OppNets. As a case study, integrate our proposed framework with PROPHET, and demonstrate its effectiveness against "black hole" attacks through experimental study. The drawbacks of this paper adversary may mount another kind of attack, where he frequently moves in and out of the communication range of the destination.

F. Li et. al., [5] In this paper author proposed the impact of the blackhole attack and its differences in DTN routing. Here introduced the concept of encounter tickets to secure the evidence of each contact. In our scheme, nodes adopt a unique way of interpreting the contact history by making observations based on the collected encounter tickets. Then, following the Dempster-Shafer theory, nodes form trust and confidence opinions towards the competency of each encountered forwarding node. The drawbacks of this paper restrictions of connectivity are invalid due to high mobility and a dynamic topology.

Y. Guo et. al., [6] In this paper author proposed a misbehavior detection system to defend against blackhole and grayhole attacks. By collecting and securely exchanging data of previous encounters, a node can assess the trustworthiness of other nodes in order to detect blackhole and grayhole attacks. The experimental results through extensive simulations using different DTN routing protocols. Our simulation results show that even when the drop probability of grayhole attacks varies in a wide range,

our approach can still efficiently detect evil nodes with a high detection rate and a low false positive rate while maintaining a low energy consumption. The drawbacks of this paper MDS is designed to only detect black hole attacks.

Q. Li et. al., [7] In this paper author proposed a distributed scheme to detect packet dropping in DTNs. In our scheme, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. The drawbacks of this paper a node may move away right after forwarding the packet to its neighbor, and thus cannot overhear if the neighbor forwards the packet. The packet has multiple replicas, it is difficult for the source to verify which replica is acknowledged since there is no persistent routing path between the source and destination in DTNs.

Hesiri et. al., [8] In this paper author proposed security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability, it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. This approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. The drawbacks of this paper a predefined value based black hole identification.

Ali Dorri [9] In this paper author proposed an approach to detect and eliminate cooperative malicious nodes in MANET with AODV routing protocol. A data control packet is used in order to check the nodes in selected path; also, by using an Extended Data Routing Information table, all malicious nodes in selected path are detected, then, eliminated from network. For evaluation, our approach and a previous work have been implemented using Opnet simulator in different scenarios. The simulation results, the proposed approach decreases packet overhead and delay of security mechanism with no false positive detection. In addition, network throughput is improved by using the proposed approach. The drawbacks of this paper the cooperative black hole attack, malicious nodes can send data packets between each other in order to bypass the promiscuous based on attacker security approaches.

Jhaveri et. al., [10] In this paper author propose Blackhole and Grayhole attacks are such attacks that drop significant number of packets by performing packet forwarding misbehavior and breach the security to cause denial of service in Mobile Ad-hoc Networks (MANETs). In this paper, we discuss our previous work, R-AODV, to detect and isolate multiple Blackhole and Grayhole nodes during route discovery process and propose a modified version to improve the performance of MANET. We analyze the proposed solution and evaluate its performance using Network Simulator-2 (NS-2) under different network

parameters. The drawbacks of this paper Consumes more energy and Does not support directional antennas.

Dhurandher et. al., [11] In this paper author decried the such attack exploiting this trustworthiness is called the Black Hole attack wherein the Black Hole in the network promises routing of the data packet to the destination while in actuality it drops them hence decreasing reliability. Here analyses MANETs under single and collaborative Black Hole attack and prevent it by diverting traffic from the Black Hole. The MANETs so discussed employ the AODV routing protocol and the method so proposed is based on sending confirmation packets that are verified by the destination to check for Black Hole presence in the GAODV routing protocol so proposed. The GAODV algorithm was then simulated in both static as well as mobile node environment and it was observed that its data delivery ratio is significantly better than the conventional AODV. The drawbacks of this paper algorithm suffered from a huge time delay, unnecessary when the path is not black hole struck.

Mishra et. al., [12] The author proposed a mechanism to mitigate single black hole attack as well as cooperative black hole attack to discover a safe route to the destination by avoiding attacks. Here proposed an approach for better analysis and improve security of AODV, which is one of the popular routing protocols for MANET. Our scheme is based on AODV protocol which is improved by deploying Advanced DRI table with additional check bit. The Simulation on NS2 is carried out and the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection and elimination of the attack and maximizing network performance by reducing the packet dropping ratio in network. The drawbacks of this paper this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. Wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication.

I. Nath, et. al., [13] In this paper author proposed black hole attack is one kind of routing disturbing attacks and can bring great damage to all clusters of a MANET. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, and infrastructure-less property. As a result, an efficient algorithm to detect black hole attack is important. This paper proposes and evaluates strategies to detecting black hole attacks and build reliable and secure inter cluster routing in wireless ad hoc networks. The drawbacks of this paper only work on small network topology and single black hole node identification.

Bindra, G.S et. al., [14] In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes. In this paper, we present a mechanism to detect and remove the above two types of malicious nodes. Our proposed technique works as follows. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted(unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with

RREP for the Restricted IP(RIP)also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes the drawbacks of this paper for the false positives may occur and the algorithm may report that a node is misbehaving, when in fact it is not.

Weerasinghe, H et. al., [15] In this paper author proposed a solution to identifying and preventing the cooperative black hole attack. Our solution discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. In this paper, via simulation, we evaluate the proposed solution and compare it with other existing solutions in terms of throughput, packet loss percentage, average end-to-end delay and route request overhead. The experiments show that (1) the AODV greatly suffers from cooperative black holes in terms of throughput and packet losses, and (2) our solution proposed in [9] presents good performance in terms of better throughput rate and minimum packet loss percentage over other solutions, and (3) our solution proposed in can accurately prevent the cooperative black hole attacks. The example findings are: (1) the proposed scheme presents 5-8% more communication overhead of route request; and (2) The secure route discovery delay slightly increases the packet loss percentage. The drawbacks of this paper route discovery delay slightly increase the packet loss percentage.

## VI. CONCLUSION

There are many techniques used for finding attacker nodes in manets for efficient routing of forwarding. The black Hole attack is type of attack in the mobile ad-hoc network which is to continuously drop or eavesdrop the message while route discovery. The Gray Hole attack is another type of attack in the mobile ad-hoc network which is to time period based drop or eavesdrop the message while route discovery. In many existing systems improve the packet sending but no one can identify the exact malicious node. Still MANET networks constitute a challenge regarding security problem due to changing topology and attacks. So, this is very dangerous attack which if never detected timely can leads to decrease the performance of our network and the loss of our sensitive data.

## REFERENCES

- [1] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in Proc. 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Comput., 2007, pp. 1–8.
- [2] Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2010, pp. 1–6.
- [3] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.
- [4] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Elsevier J. Ad Hoc Netw., vol. 14, pp. 1497–1509, 2013.
- [5] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," in Proc. INFOCOMM, 2009, pp. 2428–2436.
- [6] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., Jan. 2013, pp. 1–7.
- [7] Q. Li and G. Cao, "Mitigating routing misbehaviors in disruption tolerant networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 664–675, Apr. 2012.
- [8] Hesiri Itserasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, 2008, pp.39-54.
- [9] Ali Dorri "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET" Wireless Networks pp 1–12 Springer Science Business Media New York 2016
- [10] Jhaveri, R. H. "MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs". In Third international conference on advanced computing and communication technologies (ACCT). 2013
- [11] Dhurandher, S. K., Woungang, I., Mathur, R., & Khurana, P. "GAODV: A modified AODV against single and collaborative black hole attacks in MANETs". In 27th international conference on advanced information networking and applications workshops (WAINA). March 2013
- [12] Jaiswal, Ranjeet, and Sanjay Sharma. "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network." In Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp. 499-504. IEEE, 2013
- [13] Nath, I., & Chaki, R. (2012). BHAPSC: A new black hole attack prevention system in clustered MANET. International Journal of Advanced Research in Computer Science and Software Engineering, 2(8), 113–121.
- [14] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "Detection and Removal of Cooperative Blackhole and Grayhole Attacks in MANETs" IEEE International Conference on System Engineering and Technology September 11-12, 2012, andung, Indonesia.
- [15] H. Weerasinghe and H. Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.